



Privacy Impact Assessment

for

Social Media Websites and Applications

Date: May 2011

Point of Contact: Kristen Lefevre

System Owner: Privacy Safeguards Division, PIRMS

Office of Management  
U.S. Department of Education

## 1. **Introduction**

The Department of Education (“the Department” or “ED”) uses various social media websites, tools, and applications to engage in dialogue, share information, and collaborate with others. While non-governmental third-parties control and operate many of these sites, some are controlled and operated by ED.

The term “social media,” also referred to as social networking, Web 2.0, or Gov 2.0, describes media designed for dissemination over websites through social interaction, and created using highly accessible and scalable publishing techniques. Social media focuses on the ability of people to collaborate and share information online. It is an enabling platform for Web-based communities of interest, collaboration, and interactive services. Through social media, people or groups can create, organize, edit, comment on, combine, and share content of mutual interest.

This Privacy Impact Assessment (PIA) covers all of ED’s current, authorized social media websites and applications that are functionally comparable with substantially similar practices across each website and application. This includes those owned by ED or by a third-party.

ED will prepare a separate PIA for any social media use that raises distinct privacy risks from those covered by this PIA. The social media websites and applications covered by this PIA do not solicit, collect, maintain, or disseminate sensitive personally identifiable information (PII) from individuals who interact with these authorized social media websites and applications.

ED is using third-party social media sites to provide ED content in formats that may be useful or interesting. However, [www.ed.gov](http://www.ed.gov) is the official source of information from the U.S. Department of Education. Using these third-party sites does not constitute an endorsement by ED or any of its employees of the sponsors of the sites or the information or products presented on the sites. Additionally, please be aware that the privacy protections provided at [www.ed.gov](http://www.ed.gov) may not be available on third-party sites and applications.

Due to the dynamic nature of social media, this PIA will not list ED’s authorized social media websites and applications. An updated list of ED’s current social media presence can be found at <http://www2.ed.gov/about/overview/focus/social-media.html>.

## 2. **Legal Authority. Cite the legal authority to collect and use this data.**

The President’s Memorandum on Transparency and Open Government (January 21, 2009) and the Director of the Office of Management and Budget’s (OMB) Open Government Directive Memorandum (December 8, 2009), direct agencies to harness new technologies to engage the public and provide concrete steps to implement the system of transparency, participation, and collaboration. They also encourage the solicitation of public feedback to identify information of the greatest use to the public, assess and improve levels of collaboration, and identify new opportunities for cooperation in government.

In response to this Memorandum, ED developed its Open Government Plan. <http://www.ed.gov/open/plan>. This plan encourages public participation using web-based collaboration tools and will use such tools to engage the public. Accordingly, the Department uses social media websites or applications for external relations (such as communications, outreach, and public dialogue), to provide information about or from the Department, to encourage citizen participation, engagement, and collaboration, to provide a new channel for ED to broadcast core messages targeted at the ED community and to provide customer service. The Department uses these tools to make information and services widely available, while promoting transparency and accountability. Any information that ED places on a social media website or application will also be made available through ED's official website ([www.ed.gov](http://www.ed.gov)), or other official means, whenever possible.

The Department also has authority to perform “public information functions, including the provision, through the use of the latest technologies, of useful information about education and related opportunities to students, parents, and communities.” 20 U.S.C. Section 3412(e) (2).

Although ED uses social media websites and applications, it does not actively seek sensitive PII, nor does it collect, maintain, or disseminate sensitive PII from individuals who interact with its authorized social media websites and applications. In very limited circumstances, ED may use the minimum amount of non-sensitive PII that it receives if that information is necessary for the proper performance of agency functions and has practical utility. OMB Circular A-130. For example, if a user provides an e-mail address, which may or may not identify the individual, and requests the Department to respond, ED may use the e-mail address to do so, but only for that purpose.

**3. Purpose of ED's Use of the Social Media Tool. State the specific purpose of the use of the third-party or ED social media website or application.**

The Department may utilize social media websites or applications for external relations (such as communications, outreach, and public dialogue), to provide information about or from the Department, to encourage citizen participation, engagement, and collaboration, to provide ED with a new channel to broadcast its core messages targeted at its stakeholders, and to provide customer service. The Department uses these tools to make information and services widely available, while promoting transparency and accountability. Any information that ED places on a social media website or application will also be made available through ED's official website ([www.ed.gov](http://www.ed.gov)), or other official means, whenever possible. If ED uses social media to solicit feedback, ED will provide an alternative government e-mail address where users can also submit feedback, whenever possible.

For all social media websites and applications that this PIA covers, ED is not permitted to actively seek sensitive PII, and may only use the minimum amount of PII necessary, such as voluntarily provided contact information, for the proper performance of agency functions and which has practical utility. OMB Circular A-130. The social media websites and applications covered by this PIA are functionally comparable, with substantially similar practices across each website and application.

**4. Characterization of the Information. What elements of PII are likely to become available to the agency through public use of the website or application?**

Although many third-party social media websites and applications collect PII (e.g., name, DOB, age, etc.) to establish a user account for registration and other purposes, ED does not have access to this data, and does not directly or indirectly collect, maintain, or disseminate sensitive PII from individuals who interact with any authorized third party or ED-controlled social media website or application. The Department encourages users to consult the representatives of any third-party controlled and operated service provider to be informed of the PII collection and maintenance policies on these social media websites.

Upon registration, users select a level of interaction and how much visibility they want to have through social media websites or applications. Users may place comments, messages, and other information on the websites' public spaces. The extent of PII revealed by the user is completely at his or her discretion and as such cannot be fully characterized. At times, users may voluntarily provide contact information, such as an e-mail address, which may or may not identify the individual, for ED staff to follow-up. Where possible, ED prominently discourages the posting of sensitive PII and may also delete any sensitive PII that is posted, of which we become aware and to the extent possible. If PII is so posted, ED reserves the right to purge PII, as it does not meet our posting standards.

ED does not intend to collect information under the Paperwork Reduction Act. If it decides to do so, another PIA will be developed to assess that usage.

**5. Uses of the Information. What is the intended or expected use of the information?**

While ED does use social media websites and applications as platforms for communicating its message to reach as many people as possible or to target specific audiences (i.e., students, teachers), ED does not collect, maintain, or disseminate sensitive PII from individuals who interact with any authorized ED social media website or application. To the extent possible, ED will review the postings to social media websites and applications to fulfill the purposes of using the website or application. For example, if ED requests comments about what questions the Secretary will answer at an education summit or for ideas for reaching out to a certain student population, postings will be reviewed for that purpose.

While ED does not actively seek sensitive PII, ED may only use the minimum amount of non-sensitive PII which it receives that is necessary for the proper performance of agency functions and which has practical utility. OMB Circular A-130. For example, if a user provides contact information and requests that the Department respond, ED is permitted to use the contact information to do so. However, if such contact information is provided, ED will use it only for the purpose for which it was provided, i.e., follow-up for the specific reason that the user requested. Additionally, ED will collect and maintain such information in compliance with applicable laws and regulations, such as the Privacy Act, the Paperwork Reduction Act, and the Federal Records Act.

**6. Sharing and Disclosure. With which organizations will the information be shared?**

The information that users voluntarily post on social media websites and applications will be available to the third-party provider and any users on a social media website or application who are able to access the public-facing side of an account. The Department may share information posted on an ED-sponsored page internally if there is a demonstrated need to know, such as a user-requested follow-up. ED will only post information after it has been appropriately approved and vetted by appropriate ED officials.

For third-party social media websites and applications, information posted is considered to be public by its very nature. By choosing to post information, the user has voluntarily chosen to share this information publicly. ED does not own or control the third-party sites, and accesses them as a user. The public will have access to content posted and published by ED staff to the third party social media site. In addition, the public will be able to submit comments or questions about the posted content using the comment capabilities provided by the social media website or application.

**7. Information maintenance. Whether and how the agency will maintain PII, and for how long.**

ED does not solicit sensitive PII and does not collect, maintain, or disseminate sensitive PII from individuals who interact with its authorized social media websites and applications. Sensitive PII is not an acceptable posting to any ED-operated or authorized site. ED will therefore not “receive” such information, as it is defined in the Federal Records Act. Because it is then not a Federal Record, ED reserves the right to purge the sensitive PII.

If non-sensitive PII, such as voluntarily provided contact information, is posted to an ED-operated or authorized site in connection with the transaction of public business, it may become a Federal record. If so, ED will comply with the provisions of the Federal Records Act for any Federal records meeting the statutory definition, as well as any other applicable Federal law or regulation.

ED is currently developing a records schedule for Federal records that are posted to social media websites. Until the records schedule is approved, records are maintained indefinitely, i.e., will be left on the social media site.

**8. Notice. Is notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)?**

ED-operated social media websites and applications will provide individuals who interact with any authorized ED social media website and applications accounts with notice about what information will be collected.

ED will also provide notice on its authorized third-party hosted social media website and applications accounts stating explicitly that these accounts are not part of the Department’s government-operated website, where possible. Third-party social media websites and applications are not under the Federal government’s jurisdiction and are not owned and operated

by ED. To the extent practicable, ED will add its seal or emblem to its profile page on the social media website to indicate that it is an official Department presence. Users may have access to their information through their user accounts established on these third-party websites and applications. For additional information, ED recommends that users inform themselves about the privacy policies of the third-party services to which they subscribe. Such sites usually prominently post privacy policies on their homepages.

Any user interaction with ED-authorized third-party social media websites and applications is entirely voluntarily and therefore, any information displayed is provided voluntarily by users.

#### **9. Security. How ED will secure the PII it uses or maintains from Social Media Websites and Applications.**

ED does not actively seek sensitive PII and it does not collect, maintain, or disseminate sensitive PII from individuals who interact with its authorized social media websites and applications. The decision to authorize social media usage is a business decision and comes from a risk management process made by the management team with inputs from all stakeholders, including the Chief Information Officer, the Chief Information Security Officer, the Office of the General Counsel, the Chief Privacy Officer, the Office of Communications and Outreach, and the program owner. After a decision is made to authorize a social media use, the appropriate security safeguards will be implemented.

Security safeguards for third-party sites are described within the terms of use published by the third-party social media public networks. External, non-Federal, organizations operate and control third-party social media websites and applications. ED provides clear and conspicuous notice in a prominent location at the point of dissemination that these third-party social media websites and applications are controlled and operated by a third-party and is not a Federal or agency website. For third-party websites where ED maintains an official presence, and where possible, ED will provide a link to ED's privacy policy found at [www.ed.gov](http://www.ed.gov).

ED secures its own social media sites as follows:

- All physical access to Department sites are controlled and monitored 24/7 by security personnel who ensure that all persons entering the building are properly badged to enter the building.
- The computer systems employed by ED offer a high degree of resistance to tampering and circumvention. The Department uses special software programs for monitoring network traffic to identify unauthorized attempts to upload or change information, or otherwise to cause damage to this government computer system. These programs collect no information that would directly identify individuals, but they do collect information that could help ED identify someone attempting to tamper with the Web site.

#### **10. Privacy Risks. What other privacy risks exist and how ED mitigates those risks.**

**Disclosure of PII by users:** When interacting with the Department or others on a social media website (e.g., posting comments), PII that users share or disclose will ordinarily become available to other users or anyone else with access to the site. Most users will likely avoid disclosing particularly sensitive or confidential PII (e.g., Social Security or credit card number), which could be used by itself, or with other available information, to commit fraud or identity theft, or for other harmful or unlawful purposes. However, to help reduce those risks, ED will monitor postings to its authorized social media websites and applications to the extent practicable and will delete such posts of which ED becomes aware. Despite such efforts, the information may remain available elsewhere on the website, and others may have already viewed or copied the information. Additionally, ED does not request or collect any sensitive personal information nor does it conduct any official business transactions on social media applications. Where possible, ED will also provide appropriate notice to users on the third-party website itself, warning them to avoid sharing or disclosing any sensitive PII when interacting with the agency on the website. Users should also review the privacy policies of any third-party social media providers to determine if they wish to utilize that social media.

**Third-party advertising and tracking.** A third-party website operator may display advertising or other special communications on behalf of other businesses, organizations, or itself when a user interacts with the Department on the website. If the user clicks on the advertisement or reads the communication to learn about the advertised product or service, the user's PII may be shared by the website operator with the advertiser. The user's actions may also initiate tracking technology (e.g., "cookies," "web bugs," "beacons"), enabling the website operator or advertiser to create or develop a history or profile of the user's activities. The tracking data can be used to target specific types of advertisements to the user (i.e., behavioral advertising), or it can be used or shared for other marketing or non-marketing purposes. Users can avoid or minimize these risks by not clicking on advertisements or not visiting advertisers' sites.

**Spam, unsolicited communications, spyware, and other threats.** Users may also receive spam or other unsolicited or fraudulent communications as a result of their interactions with the Department on third-party websites. To avoid harm, users should be wary of responding to such communications, particularly those that may solicit the user's personal information, which can be used for fraudulent or other undesirable purposes. Users should also avoid accepting or viewing unknown or unsolicited links, applications, or other content that may be sent or forwarded in such communications. These unsolicited links and applications can contain unwanted tracking technology as well as computer viruses or other malicious payloads that can pose a variety of risks to the user. Where possible, ED will also provide warnings about these risks in notice(s) to users on the Department's third-party website itself.

**Accounts or pages that misrepresent agency authority or affiliation.** Certain accounts or pages on the website may not be officially authorized by, or affiliated with, ED, even if they use official insignia or otherwise appear to represent ED or the Federal Government. Interacting with such unauthorized accounts or pages may expose users to the privacy or security risks described above. ED will make every reasonable effort to label or identify its account or page in ways that would help users distinguish it from any unauthorized accounts or pages. ED will also, where appropriate, inform the website operator about any unofficial accounts or pages purporting to represent ED, seek their removal, and warn users about such accounts or pages. In addition,

where possible, ED's account or page will explain that the Department does not own, operate, or control the host website, and will provide users with a direct link to ED's official Web site <http://www.ed.gov/> if users would rather not use the third-party website to communicate with ED.

**External links and embedded third-party applications.** If ED posts a link that leads to a third-party website or any other location that is not part of an official government domain, where possible, ED will provide notice to the visitor, explaining that visitors are being directed to a nongovernment website that may have different privacy policies (and risks) from those of ED's official website. Likewise, if ED incorporates or embeds a third-party application, separate from any applications that may be incorporated or embedded by the website operator itself, ED will disclose and explain the nature or extent, if any, of the third party's involvement in ED's use of the application(s). ED will also describe the use of these application(s) its own privacy policy.

**Monitoring future requirements and future technology.** In addition to the measures described above, ED will establish and/or maintain procedures to identify, evaluate, and address any new additional privacy requirements that may result from new statutes, regulations, or policies. Second, ED will evaluate the privacy risks of any new technologies before deciding whether to adopt it. Third, ED will monitor research or trends in privacy protection technologies or policies that may facilitate new approaches to avoiding or mitigating privacy risks and better protecting PII.

**Monitoring the third-party website's privacy policies.** Prior to using a third-party social media website or application, ED will examine the third-party website's privacy policy to evaluate the risks and determine that the site is appropriate for ED's use. To the extent practicable, ED will monitor any changes to the website's privacy policies and periodically reassess the risks.

#### **11. Privacy Act System of Records. Whether ED's activities will create or modify a "system of records" under Privacy Act, 5 U.S.C. 552a?**

A system of records will not be created or altered for authorized ED social media websites or applications because the records are not retrieved by a unique individual identifier. Therefore, authorized ED social media websites and applications are not categorized as systems of records as defined by the Privacy Act.